REMARKS

Claims 1-36 are pending in the present application as amended. Independent claims 1, 9, 19, and 27 have been amended. No claims have been canceled or added. Applicants respectfully submit that no new matter has been added.

Telephone Conversation With Examiners

Applicants' representative thanks Examiners Lai and Dalencurt for the telephone discussion conducted on January 23, 2008. Proposed claim amendments were discussed in view of the cited art. Applicants' representative agreed to a claim amendment directed to the authenticator being a separate entity from the resource provider and the resource requester. Further, Applicants' representative indicated that it appeared that a difference between Applicants' claimed invention and the cited art was that in the cited art, content is available to a player in a protected form, but is renderable only if the agent so allows. In contrast, in accordance with Applicants' claims, content is provided by a resource provider only upon concluding that the resource requester can be trusted. The examiners agreed to consider this upon examination.

Claim Rejections Under 35 U.S.C. § 102

Claims 1-5, 9-15, 19-23, and 27-33 are again rejected under 35 U.S.C. § 102(e) as being anticipated by Rothrock (U.S. Pat. No. 7,174,320). Applicants respectfully traverse the Section 102 rejection insofar as it may be applied to the claims as amended.

As was previously pointed out, the present invention is generally directed toward the situation where some entity on a computer requires a resource from a software or hardware electronic entity that has been designated as the resource provider (RP), and because of the sensitive nature of the resource, the RP needs to be able to establish trust in the entity, which has been designated the resource recipient (RR). For example, the RP can be a server or some other source of sensitive data, such as for example a data vault with a sensitive document, and the RR can be a rendering entity that renders an output based on the data, such as a word processor that is to edit or print the sensitive document.

Accordingly, the RP should only provide the resource to the RR if the RR can be authenticated. In the present invention, it is presumed that the RR includes sensitive security information in what has been designated an 'id', and a value designated as a 'code-ID' may be calculated from the RR and the id thereof, perhaps as a hash, where the RP will only provide the resource to the RR if, among other things, an expected code-ID is calculated for the RR. Thus, if the RR or the id thereof are modified, the code-ID calculated therefrom will differ from that which the RP expects, and the RP will refuse to provide a requested resource based on such a differing code-ID.

In particular, in the present invention as recited in independent claim 1, an RR operating on a computing device requests a resource from an RP that is a software or hardware electronic construct, and the RR has an id that includes security-related information specifying an environment in which the RR operates. The RR and the id are loaded onto the computing device and a corresponding code-ID is calculated based on the RR and id. The RR requests the resource from the RP, and an authenticator that is separate from the RR and the RP ascertains that the requesting RR has rights to the resource and is to be trusted with the resource.

In addition, the request for the resource is forwarded by the authenticator to the RP, and includes the calculated code-ID for the requesting RR, the id for the requesting RR, and a definition of the resource requested by the RR. Thus, the RP verifies that the calculated code-ID in the forwarded request matches one of one or more valid code-IDs for the identified RR, concludes based thereon that the RR can be trusted as being a known RR that can be presumed to be trustworthy, and also that the security-related information upon which the RR operates is known security-related information that can be presumed to be trustworthy, and responds to the forwarded request by providing the requested resource only upon so concluding. Upon receiving same, the RR employs the resource in a manner consistent with the trust imparted to the RR by the RP, and in accordance with the security-related information set forth in the id corresponding to the RR.

Independent claim 9 recites subject matter similar to that of claim 1, but from the point of view of the RP. In particular, in claim 9, the RP verifies the received request, obtains

the code-ID, the id, and the definition of the resource requested from the received request, identifies the RR and obtains each of one or more valid code-IDs for the identified RR, and verifies that the calculated code-ID in the received request matches one of one or more valid code-IDs for the identified RR. With such verification, the RP can then conclude that the RR can be trusted as being a known RR that can be presumed to be trustworthy, and also that the security-related information upon which the RR operates is known security-related information that can be presumed to be trustworthy.

Independent claims 19 and 27 recite subject matter similar to that of claims 1 and 9, respectively, although in the form of a computer-readable medium with computer-executable instructions for performing the respective methods.

The Rothrock reference discloses a player such as a digital media player that accesses content, where a content license associated with the content is examined to determine if such access is permitted. Specifically, the player is on a computing device and is examined by an agent on the computing device to determine that the player is authentic based on identifying and security information relating to the player, and if so the player then obtains and renders the content in accordance with the content license and the security information. That is, the player employs the agent to examine the license and determine the validity thereof, and also to determine if minimum security standards set by the license exist with regard to the security information of the player. If so, the agent allows the player to render the content, and if not, the agent does not so allow.

Significantly, the content in the Rothrock system has no specific source, and certainly not any source that is a resource provider separate from a resource renderer (player) and an authenticator (agent), as is required by claims 1, 9, 19, and 27. More specifically, the Rothrock reference does not disclose or even suggest such a resource provider (RP) that responds to such an authenticator by verifying that the calculated code-ID in a received request matches one of one or more valid code-IDs for the identified RR and concluding based thereon that the RR can be trusted as being a known RR that can be presumed to be trustworthy, and also that the security-related information upon which the RR operates is known security-related information that can be presumed to be trustworthy, and responds to

the forwarded request by providing the requested resource only upon so concluding, also as is required by claims 1, 9, 19, and 27.

In the Rothrock reference then, content is freely available to a player (resource requester) in a protected form, but is renderable only if the agent (authenticator) so allows. In contrast, in the present invention as recited in claims 1, 9, 19, and 27, the content is provided by a resource provider only upon concluding that the resource requester can be trusted.

Applicants respectfully note that the Examiner attempts to make an argument that the resource provider recited in the claims is supplied in the Rothrock reference by a Rothrock user. However, Applicants respectfully point out that such Rothrock user is not a resource provider that is a software or hardware electronic construct, as is now recited in claims 1, 9, 19, and 27. In any event, such a Rothrock user is not specified as providing content only if such user imparts trust to the Rothrock player in the manner recited in claims 1, 9, 19, and 27.

Accordingly, for all of the aforementioned reasons, Applicants respectfully submit that the Rothrock reference does not anticipate claims 1, 9, 19, or 27, or any claims depending therefrom, including claims 2-5, 10-15, 20-23, and 28-33. As a result, Applicants respectfully request reconsideration and withdrawal of the Section 102 rejection.

Claim Rejections Under 35 U.S.C. § 103

Claims 6-8, 16-18, 24-26, and 34-36 are rejected under 35 U.S.C. § 103(a) as being obvious over the Rothrock reference in view of Mourad et al.(U.S. Pat. No. 7,171,558). Applicants respectfully traverse the Section 103 rejection insofar as it may be applied to the claims as amended.

Applicants respectfully note that inasmuch as independent claims 1, 9, 19, and 27 have been shown to be unanticipated and are non-obvious, then so too must all claims depending therefrom be unanticipated and non-obvious, including such claims 6-8, 16-18, 24-26, and 34-36, at least by their dependencies. As a result, Applicants respectfully request reconsideration and withdrawal of the Section 103 rejection.

In view of the foregoing Amendment and Remarks, Applicants respectfully submit that the present application including claims 1-36 is in condition for allowance and such action is respectfully requested.

Respectfully submitted,

Date: February 15, 2008

/Joseph F. Oriti/
Joseph F. Oriti
Registration No. 47,835

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439